⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭60－247683

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和60年(1985)12月7日
G 09 C 1/00		7368－5B	
// G 06 F 12/16		7737－5B	
H 04 L 9/02		A－7240－5K	審査請求　未請求　発明の数 1　（全4頁）

㊹発明の名称　データ保護管理システム

㉑特　願　昭59－104228

㉒出　願　昭59(1984)5月23日

㉒発明者　滑川　敏彦　吹田市山田丘2番1号　大阪大学工学部内

㉒発明者　笠原　正雄　吹田市山田丘2番1号　大阪大学工学部内

㉒発明者　常盤　欣一郎　吹田市山田丘2番1号　大阪大学工学部内

㉒発明者　松見　知代子　吹田市山田丘2番1号　大阪大学工学部内

㉒発明者　西門　裕　神戸市兵庫区和田崎町1丁目1番2号　三菱電機株式会社制御製作所内

㉒発明者　藤井　正泰　神戸市兵庫区和田崎町1丁目1番2号　三菱電機株式会社制御製作所内

㉑出願人　三菱電機株式会社　東京都千代田区丸の内2丁目2番3号

㉔代理人　弁理士　田澤　博昭　外2名

明　細　書

1. 発明の名称

データ保護管理システム

2. 特許請求の範囲

(1) 情報を分散管理するシステムにおいて、多項式版に拡張された中国人の剰余定理に基づき元の情報を複数の分割情報としてそれぞれ符号化し、符号化された前記分割情報の中から任意の一定個数以上の分割情報を集めて元の情報列を一意に復号化するようにしたことを特徴とするデータ保護管理システム。

(2) 一定個数以上の分割情報を集めて復号化された元の情報列は論理的に正しく再生されているかどうか判定されたものであることを特徴とする特許請求の範囲第1項記載のデータ保護管理システム。

3. 発明の詳細な説明

〔発明の技術分野〕

この発明は、情報の分散管理及びデータを暗号化して保護する方式に関するものである。

〔従来技術〕

従来、この種の暗号化方式として、米国のデータ暗号化規格（ＤＥＳ）や公開鍵暗号方式がある（例えば土居範久著、"米国のデータ暗号化規格ＤＥＳ"，コンピュータ・サイエンス、bit Vol. 13，№2，P4～P15共立出版（1981）参照）。

米国のデータ暗号化規格（ＤＥＳ）は、元の情報列を64ビット毎のブロックに分割してそれぞれを入力ブロックとし、換字及び転置処理を施すことにより、暗号化された64ビットの出力情報を作成するものである。すなわち、入力ブロックに対し、64ビットの鍵を使うことにより暗号文を作り出すものである。ＤＥＳでは暗号化の鍵と復号化の鍵は同一であるが、公開鍵暗号方式では、暗号化と復号化の鍵が異なるため、暗号化の鍵は公開される。

従来のこの種の暗号化方式は、以上のように構成されていたので、1つの暗号化された情報とそれを復号化するための鍵さえあれば、元の情報列

を容易に再生できる欠点があつた。

〔発明の概要〕

この発明は上記のような従来のものの欠点を除去するためになされたもので、元の情報列を暗号化された複数個の情報に分割し、それらの中から任意の一定個数以上の分割情報を集めると元の情報列が再生できるいわば情報と鍵を分散管理するデータ保護管理システムを提供することを目的としている。

〔発明の実施例〕

以下、この発明の一実施例を図について説明する。第1図において、1は元の情報列$f(x)$として用いるデータベース、2はN個に分割され、分散管理される分割情報、3はN個の分割情報2中K個以上より再生されるデータベース4は元の情報列$f(x)$をN個に分割する符号化器、5はK個以上の分割情報2より元の情報列$f(x)$を再生する復号器である。符号化器4は第2図に示すように並列に入力をする複数のガロアフィールド$G(F_2)$上のGF(2)除算器6からなり、復号器5は第3図に示すように、GF(2)乗算器7、GF(2)除算器8及びGF(2)乗算器9の並列回路からなり、GF(2)乗算器9の各出力を加算するGF(2)加算器10で加算して元の情報列$f(x)$を出力する。

一般に、元の情報列$f(x)$をN個に分割し、そのうち任意のK個以上を集めると元のデータが再生できるかという問題は、(K,N)しきい値問題として呼ばれている。この発明では次の整数における中国人の剰余定理を多項式版に拡張したものを適用することによりこの問題を解いている。

(a) 整数における中国人の剰余定理について説明する。

m_i($i=1,2,\cdots,r$)を互いに素である整数とし、

$$M=\prod_{i=1}^{r} m_i$$

とおく。この時、任意の整数a_i($i=1,2,\cdots,r$)が与えられるとすると、

$$f\equiv a_i \pmod{m_i}$$
$$0\leq f<M$$

を満たす整数fはただ1つ必ず存在する。

例えば、$m_1=5$, $m_2=6$, $m_3=7$とすると、$M=210$となる。

$a_1=2$, $a_2=4$, $a_3=1$とすると、$f=22$となる。

すなわち

$$\begin{cases} 22\equiv 2 \pmod 5 \\ 22\equiv 4 \pmod 6 \\ 22\equiv 1 \pmod 7 \\ 0\leq 22<210 \end{cases}$$

が成立する。

(b) 多項式における中国人の剰余定理について説明する。

$m_i(x)$($i=1,2,\cdots,N$)を互いに素であるガロアフィールド2(GF(2))上の多項式とする。

$$M(x)=\prod_{i=1}^{k} m_i(x) \quad \cdots\cdots\cdots (4)$$

とおく。

任意の多項式$a_i(x)$($i=1,2,\cdots,K$)が与えられた時、

$$\begin{cases} f(x)\equiv a_i(x) \pmod{m_i(x)} & \cdots\cdots\cdots (5) \\ \text{次数 } f(x)<\text{次数 } M(x) & \cdots\cdots\cdots (6) \end{cases}$$

を満たす多項式の元の情報列$f(x)$はただ1つ必ず存在する。

上記の多項式に拡張された中国人の剰余定理により次の関係を導くことができる。

$f(x)$を$m_i(x)$($i=1,2,\cdots,N$)で割つた余りを$a_i(x)$とする。この時、$f(x)$はN個の$a_i(x)$の中から任意に選んだK個の$a_i(x)$($i=1,2,\cdots,K$)から次のように再生できる。

$$\begin{cases} f(x)\equiv \sum_{i=1}^{k} \dfrac{M(x)}{m_i(x)}\cdot t_i(x)\cdot a_i(x), \bmod M(x) & \cdots\cdots (7) \\ \text{但し、} \\ t_i(x)は \dfrac{M(x)}{m_i(x)}\cdot t_i(x)\equiv 1, \bmod m_i(x) & \cdots\cdots\cdots (8) \end{cases}$$

これらの関係式を第1図のシステムに対応させると、$m_i(x)$はN分割を特徴づける多項式、Kは再生個数、$a_i(x)$はN個の分割情報2、$f(x)$は元の情報列に対応する。

いま、$m_i(x)$($i=1,2,\cdots,N$)がすべてd次

の多項式とすると、$f(x)$は式(4)と式(6)の関係より dK−1 次の多項式すなわち、元の情報列 $f(x)$ は dK ビットの情報量となる。また $a_1(x)$ は $m_1(x)$ で割った余りであることから、d−1 次の多項式すなわち、分割情報2は d ビットの情報量となる。従つて、各分割情報2の情報量は元の情報列 $f(x)$ のものの $1/K$ となつていることがわかる。

例えばN＝3，K＝2とすると、互いに素な4次（d＝4）のGF(2)上の多項式を3つ選ぶ。

$$m_1(x)=x^4+x+1 \quad \cdots\cdots\cdots (9)$$

$$m_2(x)=x^4+x^2+1 \quad \cdots\cdots\cdots (10)$$

$$m_3(x)=x^4+x^3+1 \quad \cdots\cdots\cdots (11)$$

もとのデータベース1の情報列をdKビット、すなわち8ビットずつブロック化し、符号化器4により分割符号化する。仮に1つのブロック化した情報列が10100011とすると、

$$f(x)=x^7+x^5+x+1$$

と表わされる。更にこの時の分割情報2は3個のGF(2)除算器6の剰余として

$$a_1(x)\equiv f(x)/m_1(x)\equiv x^3+x^2+x \rightarrow 1110 \quad \cdots (12)$$

$$a_2(x)\equiv f(x)/m_2(x)\equiv x^3+x+1 \rightarrow 1011 \quad \cdots (13)$$

$$a_3(x)\equiv f(x)/m_3(x)\equiv x^3+x^2+x+1 \rightarrow 1111 \quad \cdots (14)$$

と分割符号化される。このようにして、4ビット（元の情報列 $f(x)$ の $1/K=1/2$ の情報量）の分割情報2がN個、すなわち3個できる。これを復号する前に式(8)の $t_i(x)$ を計算しておく。

(i) 再生時に $a_1(x)$ と $a_2(x)$ を使う場合

$$t_1(x)=x^2+x+1 \quad \cdots\cdots\cdots (15)$$

$$t_2(x)=x^2+x \quad \cdots\cdots\cdots (16)$$

(ii) 再生時に $a_2(x)$ と $a_3(x)$ を使う場合

$$t_2(x)=x+1 \quad \cdots\cdots\cdots (17)$$

$$t_3(x)=x \quad \cdots\cdots\cdots (18)$$

(iii) 再生時に $a_3(x)$ と $a_1(x)$ を使う場合

$$t_3(x)=x^3+x+1 \quad \cdots\cdots\cdots (19)$$

$$t_1(x)=x^3+x^2 \quad \cdots\cdots\cdots (20)$$

最後に任意のK個の分割情報2より元の情報列 $f(x)$ を復号器5により復号する場合を説明する。

(i) $a_1(x)$ と $a_2(x)$ より復号する場合

式(7)に式(9)，(10)，(12)，(13)，(15)，(16) を代入して、

$$\left.\begin{aligned} f(x)\equiv m_2(x)t_1(x)a_1(x)+m_1(x)t_2(x)a_2(x)\equiv x^7+x^5+x+1 \\ \bmod m_1(x)m_2(x)\end{aligned}\right\} \cdots (21)$$

(ii) $a_2(x)$ と $a_3(x)$ より復号する場合

式(7)に式(10)，(11)，(13)，(14)，(17)，(18) を代入して、

$$\left.\begin{aligned} f(x)\equiv m_3(x)t_2(x)a_2(x)+m_2(x)t_3(x)a_3(x)\equiv x^7+x^5+x+1 \\ \bmod m_2(x)m_3(x)\end{aligned}\right\} \cdots (22)$$

(iii) $a_3(x)$ と $a_1(x)$ より復号する場合

式(7)に式(9)，(11)，(12)，(14)，(19)，(20)を代入して、

$$\left.\begin{aligned} f(x)\equiv m_1(x)t_3(x)a_3(x)+m_3(x)t_1(x)a_1(x)\equiv x^7+x^5+x+1 \\ \bmod m_3(x)m_1(x)\end{aligned}\right\} \cdots (23)$$

以上のように復号した結果、式(21)(22)(23)はいずれの場合も元の情報列 $f(x)$ を正しく再生し、元のデータベース1と同一内容のデータベース3を再生することができる。

式(21)の復号動作を第3図において説明する。復号器5に入力される2個の分割情報2である $a_1(x)$ 及び $a_2(x)$ は、GF(2)乗算器7により $t_1(x)$, $t_2(x)$, $t_k(x)$ と乗算され、それぞれ $t_1(x)a_1(x)$ 及び $t_2(x)a_2(x)$ となつて出力される。次に式(21)の $\bmod m_1(x)m_2(x)$ なる関係を保つためにGF(2)除算器8に入力され、$m_1(x)$, $m_2(x)$, $m_k(x)$ により除算され、それぞれの剰余が出力され、更にGF(2)乗算器9により

$\prod_{i=1,i\neq 1}^{k} m_i(x)$, $\prod_{i=1,i\neq 2}^{k} m_i(x)$, $\prod_{i=1,i\neq k}^{k} m_i(x)$ により乗算されてそれぞれ $m_2(x)t_1(x)a_1(x)$ 及び $m_1(x)t_2(x)a_2(x)$ の出力となる。最後にGF(2)加算器10によりそれらを加算した結果として元の情報列 $f(x)$ が得られる。

この発明では分割情報2が元の情報列 $f(x)$ の $1/K$ の情報量しかないため、K個未満の分割情報2からは元の情報列 $f(x)$ は正しく再生できないことは明らかである。逆に、K個を越えた分割情報からは、式(7)により、再生された元の情報列 $f(x)$ とオール"0"の情報系列から成る付属情報が得られ、この付属情報がオール"0"かどうかをチエックすることにより、元の情報列を正しく再生できたかどうかを判定することができる。

〔発明の効果〕

以上のように、この発明によれば、N個の分割情報のうち任意のK個を集めれば元の情報列が再生でき、K−1個以下では元の情報列が再生できず、更にK＋1個以上であれば元の情報列が正しく再

生できたかどうかをチエックできるので、分割された情報の機密性、分割された情報の紛失・盗難等に対する情報の再現性、分割された情報の改ざん、ノイズ誤りに対する誤り検出及び訂正能力を特徴とする新しいデータの分散管理システムを構築することができる効果がある。

4. 図面の簡単な説明

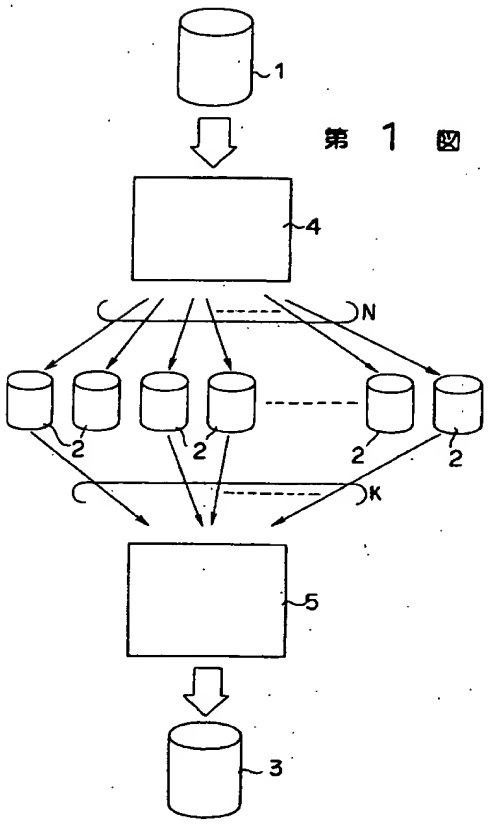
第1図はこの発明の一実施例によるデータ保護管理システムのブロック図、第2図は第1図に示す符号化器のブロック図、第3図は第1図に示す復号器のブロック図である。

1…データベース、2…分割情報、3…データベース、4…符号化器、5…復号器、6，8…GF(2)除算器、7，9…GF(2)乗算器、10…GF(2)加算器。

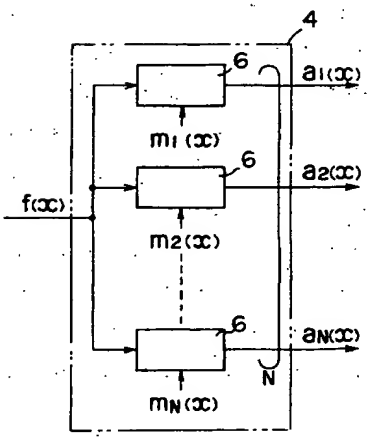
なお、図中、同一符号は同一、又は相当部分を示す。

特許出願人　三菱電機株式会社
代理人 弁理士　田　澤　博　昭
（外2名）

第1図



第2図



第3図